PRIVACY IMPACT ASSESSMENT
Office of the Chief Financial Officer
moveLINQ

Affects Members Of the Public?

Department of Energy
Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, *Department of Energy Privacy Program,* Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	May 15, 2023
Departmental Element & Site	Office of the Chief Financial Officer, DOE Headquarters - Office of the Chief Information Officer (OCIO) EITS Data Center and Cloud Services (DCCS) environment
Name of Information System or IT Project	moveLINQ
Exhibit Project UID	N/A
New PIA ☐ **Update** ☒	This is an annual update for the PIA. An updated PIA for this system will be submitted to the Chief Privacy Officer for review within twelve (12) months. Updated information has been added to reflect the current operations of this system. This PIA is also updated to reflect that this system is not collecting information from members of the public.

	Name, Title	Contact Information Phone, Email
System Owner	Phil Knopp Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-0364 Phil.Knopp@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT		
Local Privacy Act Officer	Ana Manchester Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-9360 Ana.Manchester@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Ana Manchester Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-9360 Ana.Manchester@hq.doe.gov
Person Completing this Document	Phil Knopp Office of Corporate Business Systems (CF-40) Office of the Chief Financial Officer (CF) U.S. Department of Energy	301-903-0364 Phil.Knopp@hq.doe.gov
Purpose of Information System or IT Project	MoveLINQ is a Web-based application used to generate documents associated with Permanent Change of Station moves for DOE employees. The system simplifies the expense management of government relocations and provides an intuitive user interface that allows users to easily manage and navigate through the complexities of government relocations. The system user(s) enter the appropriate information on a web-based form. Once the form is complete, the documents are printed or saved to a PDF file. Printed documents are mailed to the Permanent Change of Station (PCS) traveler for signature. PDF files are encrypted and sent to traveler via e-mail. Access is only via the DOE intranet and/or the DOE Virtual Private Network (VPN). The system is hosted in the Office of the Chief Information Officer (OCIO) Data Center and System Services (DCCS) and only available to approved, authorized employees.	
Type of Information Collected or Maintained by the System:	☐ Social Security Number (SSN) ☐ Medical & Health Information ☒ Financial Information - financial arrangements (reimbursements etc.) ☐ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☒ Date of Birth, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☐ Other	

MODULE I – PRIVACY NEEDS ASSESSMENT

Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program*, defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	N/A
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	Yes
2. Is the information in identifiable form?	Yes
3. Is the information about individual Members of the Public?	No
4. Is the information about DOE or contractor employees?	Yes ☒ Federal Employees ☐ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

MODULE I – PRIVACY NEEDS ASSESSMENT

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq. There are no other additional sources of authority for this system.
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	Individuals who relocate at the expense of the Department are required to provide the required data inputs. The information is used to approve and plan PCS and to receive reimbursement for allowable PCS expenses. "This is a voluntary process. An individual may decline to provide information; however, access to the system is dependent on voluntary disclosure."

MODULE II – PII SYSTEMS & PROJECTS	
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	Contractors are involved in the maintenance of the system. Personal information may be disclosed to these contractors and their officers and employees in performance of their contracts. The individuals provided this type of information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a. Contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	DOE has assessed moveLINQ as a moderate-risk systems according to the criteria set forth in Federal Information Processing Standard 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. moveLINQ is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls: • Strict access control enforcement based on need-to-know • All system team members are required to take a cyber security certification course before gaining access to this system The unauthorized disclosure of information is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of moveLINQ from being compromised. moveLINQ observes a number of protections to mitigate privacy risk as contemplated by the Fair Information Practice Principles (FIPPs). Users voluntarily provide their own information for the purpose of managing and working through government relocations which furthers individual participation. Contact information about individuals that relocate at the expense of the government members is required to approve and plan PCS and financial arrangements (reimbursements etc.). Individual consent is confirmed before any required actions are taken. moveLINQ emphasizes individual consent to protect individuals' privacy. moveLINQ collects only data that is required for validation and authentication purposes in compliance with data minimization and purpose specification. Any issues previously identified are evaluated and corrected consistent with Management's direction as documented within the Assessment and Authorization (A&A) process.

MODULE II – PII SYSTEMS & PROJECTS	
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	Yes. Information can be retrieved through the individual's name and a unique identifying number specific to the moveLINQ system (not the employee's SSN).
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	The system operates under the following Privacy Act systems of records: • DOE-26, Official Travel Records
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	MoveLINQ is not collecting new or additional information. The current Systems of Records do not require amendment or revision.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	MoveLINQ currently obtains data directly from the individual applying for PCS by means of the user interface forms. In addition the System Administrator is responsible for setting up the user profiles and privileges. Reference data (e.g. tax tables, Per Diem, Mileage and Tax Rates, Expense info, Accounting Parts, Load rates, etc.) are currently part of the moveLINQ application.
9. Will the information system derive new or meta data about an individual from the information collected?	No.

MODULE II – PII SYSTEMS & PROJECTS	
10. Are the data elements described in detail and documented?	Yes, data elements are described in the moveLINQ system manual, and the system provides context sensitive online documentation to support end users use of the application.
DATA USE	
11. How will the PII be used?	The system user(s) enter the appropriate information on a web-based form. Once the form is complete, the documents are printed or saved to a pdf file. Printed documents are mailed to the PCS traveler for signature. PDF files are encrypted and sent via e-mail. Access is only via the DOE intranet and/or the DOE Virtual Private Network (VPN). The system is housed and hosted in the Office of the Chief Information Officer (OCIO) Data Center and Cloud Services (DCCS) and only available to approved, authorized employees.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	N/A
13. With what other agencies or entities will an individual's information be shared?	N/A
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports may be produced to contain any of the information maintained in the system database. Types of standard reports include: • employee reports • destination reports • accounting reports (as configured in the accounting setup menu and accounting parts menu by the System Administrator) • un-submitted voucher reports • ad hoc reports
15. What will be the use of these reports?	Reports are used for administrative review, monitoring, and processing of actions related to Permanent Change of Duty Station activities by the CFO Travel Office.

MODULE II – PII SYSTEMS & PROJECTS	
16. Who will have access to these reports?	Authorized DOE users will have role-based access to the reports.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes. A user with System Administrator rights in moveLINQ would have the capability to identify the user, their Department organization, room number, and home address. For the limited use of security purposes, system audit logs are maintained to record system activity and user activity.
18. What kinds of information are collected as a function of the monitoring of individuals?	For security purposes, system audit logs are maintained to record system activity and user activity. This activity includes invalid logon attempts and access and modification to data in the system. The Operating System/Server logs maintained by the EITS environment contains IP information, this is separate from the application/database logging specific to moveLINQ.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	MoveLINQ established policies and procedures for controlling and monitoring access to the system. These are defined in the Security Plan and are compliant with privacy controls in NIST 800-53, rev 4.
DATA MANAGEMENT & MAINTENANCE	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	The system does not verify the accuracy or completeness of the DOE federal employees or authorized user (other than normal edit routines and/or drop-down menus). The data in the system is provided by the individual to whom it pertains. It is the individual's responsibility to review and determined that the information is accurate, timely and complete at the time it is provided. The authorization and voucher are reviewed and processed by different staff members. In addition, the CF-11 organization has an auditing staff to verify the voucher and the voucher is approved and signed by a management official of the program and/or field office of the person making the relocation.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	System is only maintained at DOE HQ in the EITS DCCS – though it may be accessed by authorized users from any internal DOENET access point.
Records Management	
22. Identify the record(s).	Financial transaction records related accounting. Records of financing employee relocations

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. ☐ Unscheduled X Scheduled *(cite NARA authority(ies) below)* Financial Management and Reporting Records • Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.
24. Records Contact	Sean Kennedy, Records Manager Sean.Kennedy@hq.doe.gov 240-315-6772
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Through CF's Assessment and Accreditation program and annual assessment processes, all baseline security controls have been implemented and tested as appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system was certified and accredited with full Authority To Operate and found to have mitigated risk to an acceptable level. Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access based on user responsibility and job function. These access controls are defined in the system security plan. All system team members (Federal and contractor) are required to take the DOE standard cyber security certification course as a necessary prerequisite for the system access. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include non-disclosure agreements, separation of duties so individuals only have access to appropriate pieces of personal information, and use of system audit logs to monitor access and user activity in the system.
26. Who will have access to PII data?	DOE Federal and contractor personnel have access to the data. Access to personal data in the system will be strictly controlled based on job responsibility and function.

MODULE II – PII SYSTEMS & PROJECTS	
27. How is access to PII data determined?	DOE Federal and contractor personnel who have a moveLINQ user ID are authorized registered moveLINQ users (approved by the System Owner) and will have access to the data in the system according to the user role assigned. Access to data in the system is strictly controlled based on job responsibility and function.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	N/A
30. Who is responsible for ensuring the authorized use of personal information?	System Owner, the Chief Financial Officer, and the Director for Corporate Information Systems.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	**Phil Knopp** **(Print Name)** Philip A. Knopp Digitally signed by Philip A. Knopp Date: 2023.10.03 14:14:24 -04'00' **(Signature)**	
Local Privacy Act Officer	**Ana Manchester** **(Print Name)** Ana M. Manchester Digitally signed by Ana M. Manchester Date: 2023.10.03 08:03:21 -04'00' **(Signature)**	
Chief Privacy Officer	**William K. Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.10.02 14:16:23 -04'00' **(Signature)**	